Available online at www.sciencedirect.com

SCIENCE DIRECT®

ACADEMIC PRESS

Finite Fields and Their Applications 9 (2003) 458–471

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

On the distribution of points in orbits of $PGL(2,q)$ acting on $GF(q^n)$

Harald Niederreiter[a,*] and Arne Winterhof[b]

[a] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore*

[b] *Temasek Laboratories, National University of Singapore, 10 Kent Ridge Crescent, Singapore 119260, Republic of Singapore*

Received 26 September 2002; revised 21 April 2003

Communicated by Igor Shparlinski

Abstract

We prove results on the distribution of points in an orbit of $PGL(2,q)$ acting on an element of $GF(q^n)$. These results support a conjecture of Klapper. More precisely, we show that the points in an orbit are uniformly distributed if n is small with respect to q.

Keywords: Orbits; Projective general linear group; Finite fields; Character sums

1. Introduction

Let q be a prime power, $n \geqslant 3$ an integer, and ξ a defining element of the finite field $GF(q^n)$ over $GF(q)$, i.e., $GF(q^n)$ is obtained from $GF(q)$ by adjoining ξ. The projective general linear group $PGL(2,q)$ over $GF(q)$ acts on $GF(q^n) \cup \{\infty\}$ by linear fractional transformations. We restrict the attention to the action on the element ξ. The action of the matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a,b,c,d \in GF(q), \quad ad - bc \neq 0,$$

*Corresponding author. Fax: +65-779-5452.

E-mail addresses: nied@math.nus.edu.sg (H. Niederreiter), tslwa@nus.edu.sg (A. Winterhof).

1071-5797/03/$ - see front matter
doi:10.1016/S1071-5797(03)00025-X

on ξ is given by

$$M(\xi) = \frac{a\xi + b}{c\xi + d}.$$

An orbit $orbit(\xi)$ of $PGL(2,q)$ is defined as

$$orbit(\xi) = \{M(\xi) : M \in PGL(2,q)\}.$$

Motivated by a conjecture of Klapper [5], we investigate the distribution of points in $orbit(\xi)$. More precisely, we prove upper bounds on the number of points of $orbit(\xi)$ in a restricted range of powers of a fixed primitive element $\gamma \in GF(q^n)$. A first crude bound on

$$|orbit(\xi) \cap \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}|$$

with $k \leqslant q^n - 1$ can be easily obtained. The following result is mentioned in Klapper [5] (see also [7, Proposition 1; 8, Proposition 15]).

Proposition 1. *If $1 \leqslant k \leqslant t(q^n - 1)/(q-1)$ with a positive integer $t \leqslant q-1$, then for any integer r we have*

$$|orbit(\xi) \cap \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}| \leqslant t(q^2 + q).$$

Equality holds if $k = t(q^n - 1)/(q-1)$.

Proof. Put

$$P_0 = \left\{ M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in GF(q), a \neq 0 \right\} \tag{1}$$

and

$$P_1 = \left\{ M = \begin{pmatrix} a & b \\ 1 & d \end{pmatrix} : a, b, d \in GF(q), ad - b \neq 0 \right\}. \tag{2}$$

By the definition of ξ, we obviously have

$$|orbit(\xi)| = |\{M(\xi) : M \in P_0 \cup P_1\}| = |P_0 \cup P_1| = q^3 - q.$$

Note that $\gamma^{j(q^n-1)/(q-1)} \in GF(q)$ for any integer $j \geqslant 0$. We can restrict ourselves to the case $t = 1$, since we have $M(\xi) \in \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}$ if and only if

$$\gamma^{j(q^n-1)/(q-1)} M(\xi) \in orbit(\xi) \cap \{\gamma^{r+j(q^n-1)/(q-1)}, \ldots, \gamma^{r+k-1+j(q^n-1)/(q-1)}\}.$$

If $k = (q^n - 1)/(q-1)$, then for each $M \in P_0 \cup P_1$ exactly one of the elements $\gamma^{j(q^n-1)/(q-1)} M(\xi) \in orbit(\xi)$ with $0 \leqslant j \leqslant q-2$ lies in $\{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}$. Therefore,

$$|orbit(\xi) \cap \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}| = \frac{q^3 - q}{q-1} = q^2 + q.$$

For $k < (q^n - 1)/(q-1)$ the desired upper bound is an immediate consequence. □

We can easily deduce the following corollary.

Corollary 1. *If* $t(q^n-1)/(C(q-1)) \leqslant k \leqslant t(q^n-1)/(q-1)$ *with a constant* $C \geqslant 1$, *then we have*

$$|orbit(\xi) \cap \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}| \leqslant C\frac{k(q^3-q)}{q^n-1}.$$

This result is closely connected with the conjecture of Klapper [5] that there exists a constant $C>0$ such that (if $k \geqslant (q^n-1)/(q^3-q)$)

$$|orbit(\xi) \cap \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}| < C\frac{k(q^3-q)}{q^n-1}, \tag{3}$$

where C is independent of k and n. For example, (3) with $C>2$ holds true if $k \geqslant (q^n-1)/(2(q-1))$. Our main result improves on Corollary 1 if n is small with respect to q and hence it supports Klapper's conjecture.

Theorem 1. *For any integers* r *and*

$$k \geqslant \frac{2(n-1)^2(q^n-1)(\log((q^n-1)/(q-1))+1)}{(C-1)(q^2-1)}$$

with a constant $C>1$ *we have*

$$|orbit(\xi) \cap \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}| < C\frac{k(q^3-q)}{q^n-1}.$$

The proof of Theorem 1 is based on a bound on multiplicative character sums of the form

$$\sum_{\eta \in orbit(\xi)} \chi(\eta).$$

We prove the character sum bound in Section 2 and Theorem 1 in Section 3. A more general upper bound on $|orbit(\xi) \cap \{\gamma^r, \gamma^{r+1}, \ldots, \gamma^{r+k-1}\}|$ is, in fact, shown in the proof of Theorem 1.

Besides the *multiplicative distribution* of $orbit(\xi)$ we also investigate its *additive distribution*. As the ordering $GF(q^n)^* = \{1, \gamma, \gamma^2, \ldots, \gamma^{q^n-2}\}$ corresponds to the multiplicative structure of $GF(q^n)$, the following orderings correspond to the additive structure of $GF(q)$ and $GF(q^n)$, respectively. They can be regarded as generalizations of the natural ordering $\{0, 1, \ldots, p-1\}$ of $GF(p)$ when p is a prime. If $q = p^s$ with a prime p, then let $\{b_1, b_2, \ldots, b_s\}$ be a basis of $GF(q)$ over $GF(p)$ and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be a basis of $GF(q^n)$ over $GF(q)$ with $\beta_n = 1$.

We order the elements of $GF(q)$ by

$$x_l = l_1 b_1 + l_2 b_2 + \cdots + l_s b_s, \quad 0 \leqslant l \leqslant q-1,$$

if

$$l = l_1 + l_2 p + \cdots + l_s p^{s-1}, \quad 0 \leqslant l_1, l_2, \ldots, l_s \leqslant p-1,$$

and the elements of $GF(q^n)$ by

$$\xi_l = x_{l_1}\beta_1 + x_{l_2}\beta_2 + \cdots + x_{l_n}\beta_n, \quad 0 \leqslant l \leqslant q^n - 1,$$

if

$$l = l_1 + l_2 q + \cdots + l_n q^{n-1}, \quad 0 \leqslant l_1, l_2, \ldots, l_n \leqslant q-1.$$

Analogously to Proposition 1, the following results can be easily verified. We use the facts that $orbit(\xi)$ is invariant under shifts by elements of $GF(q)$ and that $\beta_n = 1$.

Proposition 2. *If $1 \leqslant L \leqslant tq^{n-1}$ for a positive integer $t \leqslant q$, then for any $\alpha \in GF(q^n)$ we have*

$$|orbit(\xi) \cap \{\alpha + \xi_l : 0 \leqslant l \leqslant L-1\}| \leqslant t(q^2-1).$$

Equality holds for $L = tq^{n-1}$.

Corollary 2. *If $tq^{n-1}/C \leqslant L \leqslant tq^{n-1}$ with a constant $C \geqslant 1$, then we have*

$$|orbit(\xi) \cap \{\alpha + \xi_l : 0 \leqslant l \leqslant L-1\}| \leqslant C\frac{L(q^3-q)}{q^n}.$$

Bounds on the additive character sums

$$\sum_{\eta \in orbit(\xi)} \psi(\eta)$$

yield the following improvement.

Theorem 2. *For any $\alpha \in GF(q^n)$ and*

$$L \geqslant \frac{3n(n-1)q^n \log q}{(C-1)(q^2-1)}$$

with a constant $C>1$ *we have*

$$|orbit(\xi)\cap\{\alpha+\xi_l : 0\leqslant l\leqslant L-1\}|\leqslant C\frac{L(q^3-q)}{q^n}.$$

We prove the character sum bound in Section 4 and Theorem 2 in Section 5. A more general upper bound on $|orbit(\xi)\cap\{\alpha+\xi_l : 0\leqslant l\leqslant L-1\}|$ is shown in the proof of Theorem 2.

2. Multiplicative character sums

Theorem 3. *Let* ξ *be a defining element of* $GF(q^n)$ *over* $GF(q)$ *with* $n\geqslant 3$ *and* χ *be a multiplicative character of* $GF(q^n)$ *of order* q^n-1. *Then for integers* j *with* $0\leqslant j\leqslant q^n-2$ *we have*

$$\left|\sum_{\eta\in orbit(\xi)}\chi^j(\eta)\right| = \begin{cases} q^3-q, & \text{if } j=0,\\ 0, & \text{if } j\not\equiv 0 \bmod (q-1),\end{cases}$$

and

$$\left|\sum_{\eta\in orbit(\xi)}\chi^j(\eta)\right| < 2(n-1)^2(q^2-q)$$

if $0\neq j\equiv 0 \bmod (q-1)$.

Proof. For $j=0$ the result is trivial. Thus, we can assume that χ^j is a nontrivial multiplicative character of $GF(q^n)$. The character χ^j restricted to $GF(q)^*$ is trivial if and only if $j\equiv 0 \bmod (q-1)$, and we have

$$\sum_{x\in GF(q)}\chi^j(x) = \begin{cases} 0, & j\not\equiv 0 \bmod (q-1),\\ q-1, & 0\neq j\equiv 0 \bmod (q-1).\end{cases}$$

From [1, Section 3] (see also [4]) we know that

$$\left|\sum_{x\in GF(q)}\chi^j(\xi+x)\right|\leqslant (n-1)q^{1/2}.$$

Moreover, we have

$$\left|\sum_{\eta\in orbit(\xi)}\chi^j(\eta)\right|\leqslant\left|\sum_{M\in P_0}\chi^j(M(\xi))\right|+\left|\sum_{M\in P_1}\chi^j(M(\xi))\right|,$$

where the sets P_0 and P_1 are defined by (1) and (2), respectively. For the first sum we have

$$\left|\sum_{M\in P_0}\chi^j(M(\xi))\right| = \left|\sum_{\substack{a,b\in GF(q)\\ a\neq 0}}\chi^j(a\xi+b)\right|$$

$$= \left|\sum_{\substack{a\in GF(q)\\ a\neq 0}}\chi^j(a)\right|\left|\sum_{b'\in GF(q)}\chi^j(\xi+b')\right|$$

$$\begin{cases} = 0, & j\not\equiv 0 \bmod (q-1),\\ \leqslant (q-1)(n-1)q^{1/2}, & 0\neq j\equiv 0 \bmod (q-1), \end{cases}$$

and for the second sum

$$\left|\sum_{M\in P_1}\chi^j(M(\xi))\right|$$

$$= \left|\sum_{\substack{a,b,d\in GF(q)\\ b\neq ad}}\chi^j(a\xi+b)\chi^{-j}(\xi+d)\right|$$

$$\leqslant \left|\sum_{\substack{a\in GF(q)\\ a\neq 0}}\chi^j(a)\right|\left(\left|\sum_{b'\in GF(q)}\chi^j(\xi+b')\right|\left|\sum_{d\in GF(q)}\chi^j(\xi+d)\right| + q\right)$$

$$+ \left|\sum_{\substack{b\in GF(q)\\ b\neq 0}}\chi^j(b)\right|\left|\sum_{d\in GF(q)}\chi^j(\xi+d)\right|$$

$$\begin{cases} = 0, & j\not\equiv 0 \bmod (q-1),\\ \leqslant (q-1)((n-1)^2q+q+(n-1)q^{1/2}), & 0\neq j\equiv 0 \bmod (q-1). \end{cases}$$

Combining these estimates, we get the result after simple calculations. □

3. Proof of Theorem 1

We can assume that $k\leqslant q^n-1$. Let χ be a multiplicative character of $GF(q^n)$ of order q^n-1. Since

$$\frac{1}{q^n-1}\sum_{j=0}^{q^n-2}\chi^j(\zeta) = \begin{cases} 1, & \zeta = 1,\\ 0, & 1\neq\zeta\in GF(q^n)^*, \end{cases}$$

we have

$$\begin{aligned}
&|orbit(\xi)\cap\{\gamma^r,\gamma^{r+1},\ldots,\gamma^{r+k-1}\}|\\
&\quad=\frac{1}{q^n-1}\sum_{j=0}^{q^n-2}\sum_{l=r}^{r+k-1}\sum_{\eta\in orbit(\xi)}\chi^j(\eta\gamma^{-l})\\
&\quad\leqslant\frac{k(q^3-q)}{q^n-1}+\frac{1}{q^n-1}\sum_{j=1}^{q^n-2}\left|\sum_{\eta\in orbit(\xi)}\chi^j(\eta)\right|\left|\sum_{l=r}^{r+k-1}\chi^j(\gamma^{-l})\right|\\
&\quad<\frac{k(q^3-q)}{q^n-1}+\frac{2(n-1)^2(q^2-q)}{q^n-1}\left(\sum_{j'=1}^{(q^n-q)/(q-1)}\left|\sum_{l=r}^{r+k-1}\chi^{j'(q-1)}(\gamma^{-l})\right|\right)
\end{aligned}$$

by Theorem 3. By [11, Chapter 3, Exercise 11] we have

$$\sum_{j'=1}^{(q^n-q)/(q-1)}\left|\sum_{l=r}^{r+k-1}\chi^{j'(q-1)}(\gamma^{-l})\right|\leqslant\frac{q^n-1}{q-1}\left(\log\left(\frac{q^n-1}{q-1}\right)+1\right).$$

Hence,

$$|orbit(\xi)\cap\{\gamma^r,\gamma^{r+1},\ldots,\gamma^{r+k-1}\}|<\frac{k(q^3-q)}{q^n-1}+2(n-1)^2q\left(\log\left(\frac{q^n-1}{q-1}\right)+1\right)$$

for any integers $k\geqslant 1$ and r. If k satisfies the lower bound in Theorem 1, then we get

$$|orbit(\xi)\cap\{\gamma^r,\gamma^{r+1},\ldots,\gamma^{r+k-1}\}|<C\frac{k(q^3-q)}{q^n-1}.\qquad\square$$

With the abbreviation $N_1=|orbit(\xi)\cap\{\gamma^r,\gamma^{r+1},\ldots,\gamma^{r+k-1}\}|$, the proof of Theorem 1 shows that

$$\left|N_1-\frac{k(q^3-q)}{q^n-1}\right|<2(n-1)^2q\left(\log\left(\frac{q^n-1}{q-1}\right)+1\right).$$

This may be viewed as a result about the uniform distribution of orbits in certain multiplicatively defined subsets of $GF(q^n)$, in case n is small with respect to q. This result is close to a conjecture of Klapper and Goresky [7, Section 6; 8, Section VIII]. (The results of [7,8] are generalized in [6].)

4. Additive character sums

Theorem 4. *Let ξ be a defining element of $GF(q^n)$ over $GF(q)$ with $n \geqslant 3$. Let ψ be the canonical additive character of $GF(q^n)$ and denote by $Tr(X) = X + X^q + \cdots + X^{q^{n-1}}$ the trace of $GF(q^n)$ onto $GF(q)$. Then for $\mu \in GF(q^n)$ we have*

$$\left| \sum_{\eta \in orbit(\xi)} \psi(\mu\eta) \right| \begin{cases} = q^3 - q, & \mu = 0, \\ = 0, & Tr(\mu) \neq 0, \\ \leqslant (n-1)q^2 + q, & Tr(\mu) = 0, \mu \neq 0. \end{cases}$$

We prove Theorem 4 after a preliminary lemma.

Lemma 1. *If $\mu \in GF(q^n)$ with $Tr(\mu) = 0$ and $\mu \neq 0$, then we have*

$$\left| \sum_{b,d \in GF(q)} \psi\left(\frac{b\mu}{\xi + d}\right) \right| \leqslant \begin{cases} (n-2)q, & Tr(\mu\xi) \neq 0, \\ (n-3)q, & Tr(\mu\xi) = 0. \end{cases}$$

Proof. By using [9, eq. (5.7)], we obtain

$$\sum_{b \in GF(q)} \psi\left(\frac{b\mu}{\xi + d}\right) = \begin{cases} 0, & Tr(\mu/(\xi + d)) \neq 0, \\ q, & Tr(\mu/(\xi + d)) = 0. \end{cases}$$

Now we have

$$Tr\left(\frac{\mu}{\xi + d}\right) = \sum_{i=0}^{n-1} \frac{\mu^{q^i}}{\xi^{q^i} + d} = \frac{\sum_{i=0}^{n-1} \mu^{q^i} \prod_{\substack{j=0 \\ j \neq i}}^{n-1} (\xi^{q^j} + d)}{\prod_{j=0}^{n-1} (\xi^{q^j} + d)}.$$

Since the polynomial

$$F(X) = \sum_{i=0}^{n-1} \mu^{q^i} \prod_{\substack{j=0 \\ j \neq i}}^{n-1} (\xi^{q^j} + X)$$

has leading coefficient $Tr(\mu) = 0$ and the coefficient of X^{n-2} is

$$\begin{aligned} \sum_{i=0}^{n-1} \mu^{q^i} \sum_{\substack{j=0 \\ j \neq i}}^{n-1} \xi^{q^j} &= \sum_{i=0}^{n-1} \mu^{q^i} (Tr(\xi) - \xi^{q^i}) = Tr(\mu)\, Tr(\xi) - Tr(\mu\xi) \\ &= -\, Tr(\mu\xi), \end{aligned}$$

it has degree $n-2$ if $Tr(\mu\xi)\neq 0$ and degree at most $n-3$ if $Tr(\mu\xi)=0$. Since

$$F(-\xi)=\mu\prod_{j=1}^{n-1}(\xi^{q^j}-\xi)\neq 0,$$

$F(X)$ is not the zero polynomial. Hence, $F(X)$ has at most $n-2$ zeros if $Tr(\mu\xi)\neq 0$ and at most $n-3$ zeros if $Tr(\mu\xi)=0$, and so we get

$$\begin{aligned}\left|\sum_{b,d\in GF(q)}\psi\left(\frac{b\mu}{\xi+d}\right)\right| &\leqslant \sum_{d\in GF(q)}\left|\sum_{b\in GF(q)}\psi\left(\frac{b\mu}{\xi+d}\right)\right| \\ &\leqslant \begin{cases}(n-2)q, & Tr(\mu\xi)\neq 0,\\ (n-3)q, & Tr(\mu\xi)=0.\end{cases}\end{aligned}$$

□

Proof of Theorem 4. For $\mu=0$ the assertion is trivial, and so we can assume that $\mu\neq 0$. We have

$$\left|\sum_{\eta\in orbit(\xi)}\psi(\mu\eta)\right|\leqslant S_0(\mu)+S_1(\mu),$$

where

$$\begin{aligned}S_0(\mu) &:= \left|\sum_{M\in P_0}\psi(\mu M(\xi))\right| = \left|\sum_{\substack{a,b\in GF(q)\\ a\neq 0}}\psi(\mu(a\xi+b))\right| \\ &= \left|\sum_{\substack{a\in GF(q)\\ a\neq 0}}\psi(a\mu\xi)\right|\left|\sum_{b\in GF(q)}\psi(b\mu)\right|\end{aligned}$$

and

$$\begin{aligned}S_1(\mu) &:= \left|\sum_{\substack{a,b,d\in GF(q)\\ b\neq ad}}\psi\left(\mu\frac{a\xi+b}{\xi+d}\right)\right| \\ &= \left|\sum_{a\in GF(q)}\psi(a\mu)\right|\left|\sum_{\substack{b',d\in GF(q)\\ b'\neq 0}}\psi\left(\frac{b'\mu}{\xi+d}\right)\right| \\ &\leqslant \left|\sum_{a\in GF(q)}\psi(a\mu)\right|\left(q+\left|\sum_{b',d\in GF(q)}\psi\left(\frac{b'\mu}{\xi+d}\right)\right|\right).\end{aligned}$$

If $Tr(\mu)\neq 0$, then we have

$$S_0(\mu) = S_1(\mu) = 0.$$

If $Tr(\mu) = 0$, $\mu\neq 0$, then we have

$$S_0(\mu) = \begin{cases} q, & Tr(\mu\xi)\neq 0, \\ q^2 - q, & Tr(\mu\xi) = 0, \end{cases}$$

and

$$S_1(\mu) \leqslant \begin{cases} (n-1)q^2, & Tr(\mu\xi)\neq 0, \\ (n-2)q^2, & Tr(\mu\xi) = 0, \end{cases}$$

by Lemma 1. Simple calculations complete the proof. □

5. Proof of Theorem 2

We can assume that $L\leqslant q^n$. Let ψ be the canonical additive character of $GF(q^n)$. Since

$$\frac{1}{q^n}\sum_{\mu\in GF(q^n)}\psi(\mu\zeta) = \begin{cases} 1, & \zeta = 0, \\ 0, & \zeta\in GF(q^n)^*, \end{cases}$$

we have

$$\begin{aligned} &|orbit(\xi)\cap\{\alpha+\xi_l : 0\leqslant l\leqslant L-1\}| \\ &= \frac{1}{q^n}\sum_{\mu\in GF(q^n)}\sum_{l=0}^{L-1}\sum_{\eta\in orbit(\xi)}\psi(\mu(\eta-\alpha-\xi_l)) \\ &\leqslant \frac{1}{q^n}\sum_{\mu\in GF(q^n)}\left|\sum_{\eta\in orbit(\xi)}\psi(\mu\eta)\right|\left|\sum_{l=0}^{L-1}\psi(\mu\xi_l)\right| \\ &\leqslant \frac{L(q^3-q)}{q^n} + \frac{(n-1)q^2+q}{q^n}\sum_{\substack{\mu\in GF(q^n)\\ Tr(\mu)=0,\mu\neq 0}}\left|\sum_{l=0}^{L-1}\psi(\mu\xi_l)\right| \end{aligned}$$

by Theorem 4.

Next we show that

$$\sum_{\substack{\mu\in GF(q^n)\\ Tr(\mu)=0,\mu\neq 0}}\left|\sum_{l=0}^{L-1}\psi(\mu\xi_l)\right|\leqslant s(n-1)q^{n-1}\left(\frac{4}{\pi^2}\log p+1.38\right), \tag{4}$$

where $q=p^s$. If $\mu\in GF(q^n)$ with $Tr(\mu)=0$ and $\mu\neq 0$, then $\psi(\mu(\xi_l+x\beta_n))=\psi(\mu(\xi_l+x))=\psi(\mu\xi_l)$ for all $x\in GF(q)$, and so

$$\sum_{l=0}^{q^{n-1}-1}\psi(\mu\xi_l)=\frac{1}{q}\sum_{l=0}^{q^n-1}\psi(\mu\xi_l)=0.$$

If $L=L_0+L_1q^{n-1}$ with $0\leqslant L_0\leqslant q^{n-1}-1$, then we have

$$\sum_{l=0}^{L-1}\psi(\mu\xi_l)=\sum_{l_1=0}^{L_1-1}\sum_{l_0=0}^{q^{n-1}-1}\psi(\mu(\xi_{l_0}+x_{l_1}))+\sum_{l_0=0}^{L_0-1}\psi(\mu(\xi_{l_0}+x_{L_1}))=\sum_{l_0=0}^{L_0-1}\psi(\mu\xi_{l_0}),$$

and so we may restrict ourselves to the case $L\leqslant q^{n-1}-1$. Now we proceed as in the proof of [10, Lemma 3] or [12, Section 3]. Note that $\{\delta_j: 1\leqslant j\leqslant sn\}$ with $\delta_j:=b_{j_1}\beta_{j_2}$ if $j=j_1+(j_2-1)s$, $1\leqslant j_1\leqslant s$, $1\leqslant j_2\leqslant n$, is a basis of $GF(q^n)$ over $GF(p)$, i.e.,

$$\xi_l=l_1\delta_1+l_2\delta_2+\cdots+l_{sn}\delta_{sn},\quad 0\leqslant l\leqslant q^n-1,$$

if

$$l=l_1+l_2p+\cdots+l_{sn}p^{sn-1},\quad 0\leqslant l_1,l_2,\ldots,l_{sn}\leqslant p-1.$$

For $j=1,\ldots,s(n-1)$ define

$$M_j=\{\mu\in GF(q^n)^*: Tr(\mu)=0,\psi(\mu\delta_1)=\cdots=\psi(\mu\delta_{j-1})=1,\psi(\mu\delta_j)\neq 1\}.$$

Then we can write

$$\sum_{\substack{\mu\in GF(q^n)\\ Tr(\mu)=0,\mu\neq 0}}\left|\sum_{l=0}^{L-1}\psi(\mu\xi_l)\right|=\sum_{j=1}^{s(n-1)}\sum_{\mu\in M_j}\left|\sum_{l=0}^{L-1}\psi(\mu\xi_l)\right|. \tag{5}$$

Now we fix $\mu\in M_j$, $1\leqslant j\leqslant s(n-1)$, and consider the sum

$$\sum_{l=0}^{L-1}\psi(\mu\xi_l).$$

For $0\leqslant l\leqslant L-1<p^{s(n-1)}-1$ we have

$$\xi_l=l_1\delta_1+l_2\delta_2+\cdots+l_{s(n-1)}\delta_{s(n-1)},\quad 0\leqslant l_1,l_2,\ldots,l_{s(n-1)}\leqslant p-1,$$

where $l = l_1 + l_2 p + \cdots + l_{s(n-1)} p^{s(n-1)-1}$. This yields

$$\psi(\mu\xi_l) = \psi(\mu\delta_j)^{l_j} \cdots \psi(\mu\delta_{s(n-1)})^{l_{s(n-1)}}$$

with $\psi(\mu\delta_j) \neq 1$. We write

$$L - 1 = r_1 + r_2 p + \cdots + r_{s(n-1)} p^{s(n-1)-1}, \quad 0 \leqslant r_1, r_2, \ldots, r_{s(n-1)} \leqslant p - 1.$$

If $j \leqslant s(n-1) - 1$ and $(l_{j+1}, \ldots, l_{s(n-1)}) \neq (r_{j+1}, \ldots, r_{s(n-1)})$, then by fixing

$$l_1, \ldots, l_{j-1}, l_{j+1}, \ldots, l_{s(n-1)}$$

and summing $\psi(\mu\xi_l)$ over $l_j = 0, 1, \ldots, p-1$ we get 0. Therefore, in the range of summation $l = 0, 1, \ldots, L-1$ we are left with the terms $\psi(\mu\xi_l)$ for which $(l_{j+1}, \ldots, l_{s(n-1)}) = (r_{j+1}, \ldots, r_{s(n-1)})$. Thus,

$$\left| \sum_{l=0}^{L-1} \psi(\mu\xi_l) \right| = \left| \sum_{l_1, \ldots, l_j} \psi(\mu\delta_j)^{l_j} \right|, \tag{6}$$

where the last sum is over all $l_1, \ldots, l_j$ with

$$l_1 + l_2 p + \cdots + l_j p^{j-1} \leqslant r_1 + r_2 p + \cdots + r_j p^{j-1}.$$

Identity (6) holds trivially for $j = s(n-1)$ as well. If $r_j \neq 0$, then by (6) we obtain

$$\left| \sum_{l=0}^{L-1} \psi(\mu\xi_l) \right| \leqslant p^{j-1} \left| \sum_{l_j=0}^{r_j-1} \psi(\mu\delta_j)^{l_j} \right| + p^{j-1} = p^{j-1} \left| \frac{\psi(r_j\mu\delta_j) - 1}{\psi(\mu\delta_j) - 1} \right| + p^{j-1},$$

and this holds trivially for $r_j = 0$ as well. For fixed $1 \leqslant j \leqslant s(n-1)$ this yields

$$\begin{aligned} \sum_{\mu \in M_j} \left| \sum_{l=0}^{L-1} \psi(\mu\xi_l) \right| &\leqslant p^{j-1} p^{s(n-1)-j} \sum_{u=1}^{p-1} \left| \frac{\sin(\pi r_j u/p)}{\sin(\pi u/p)} \right| + p^{j-1} p^{s(n-1)-j} (p-1) \\ &\leqslant p^{s(n-1)-1} \left(\frac{4}{\pi^2} p \log p + 0.38p + 0.7 \right) + p^{s(n-1)-1} (p-1), \end{aligned}$$

where we used [12, Lemma 5] in the first step and [2, Theorem 1] in the second step. In view of (5), we have thus established (4). Simple calculations yield then the result of the theorem. □

With the abbreviation $N_2 = |orbit(\xi) \cap \{\alpha + \xi_l : 0 \leqslant l \leqslant L-1\}|$, the proof of Theorem 2 shows that

$$\left| N_2 - \frac{L(q^3 - q)}{q^n} \right| < 3n(n-1) q \log q.$$

This may be viewed as a result about the uniform distribution of orbits in certain additively defined subsets of $GF(q^n)$, in case n is small with respect to q.

6. Final remarks

If L is a power of p or more generally if we consider the distribution of $orbit(\xi)$ in subsets $\{\alpha+\zeta : \zeta \in U\}$, where U is an additive subgroup of $GF(q^n)$ of cardinality L with $U \cap GF(q) = \{0\}$, then we get the slightly better result

$$|orbit(\xi) \cap \{\alpha+\zeta : \zeta \in U\}| \leqslant C\frac{L(q^3-q)}{q^n}$$

if

$$L \geqslant \frac{((n-1)q+1)q^n}{(C-1)(q^3-q)},$$

since

$$\sum_{\substack{\mu \in GF(q^n) \\ Tr(\mu)=0, \mu \neq 0}} \left| \sum_{\zeta \in U} \psi(\mu\zeta) \right| = q^{n-1}$$

(see the proof of [14, Lemma 3.4]).

The method of this paper can also be used to investigate the distribution of $orbit(\xi)$ in subsets of the form

$$\{\alpha + l_1\delta_1 + l_2\delta_2 + \cdots + l_u\delta_u : 0 \leqslant l_i \leqslant L_i - 1, i = 1, 2, \ldots, u\},$$

where $\delta_1, \delta_2, \ldots, \delta_u$ are linearly independent over $GF(p)$ and $0 \leqslant L_1, L_2, \ldots, L_u \leqslant p-1$ (cf. [3,13, Lemma 6]).

Acknowledgments

We are grateful to Igor Shparlinski for reminding us of Klapper's conjecture and motivating us to work on it. The authors were supported by DSTA Research Grant R-394-000-011-422.

References

[1] L. Carlitz, Distribution of primitive roots in a finite field, Quart. J. Math. (2) 4 (1953) 4–10.
[2] T. Cochrane, On a trigonometric inequality of Vinogradov, J. Number Theory 27 (1987) 9–16.
[3] H. Davenport, D.J. Lewis, Character sums and primitive roots in finite fields, Rend. Circ. Mat. Palermo (2) 12 (1963) 129–136.
[4] N.M. Katz, An estimate for character sums, J. Amer. Math. Soc. 2 (1989) 197–200.

[5] A. Klapper, The distribution of points in orbits of $PGL_2(GF(q))$ acting on $GF(q^n)$, in: G.L. Mullen, P.J.-S. Shiue (Eds.), Finite Fields, Coding Theory, and Advances in Communications and Computing, Marcel Dekker, New York, 1993, pp. 430–431.
[6] A. Klapper, Partial period crosscorrelations of geometric sequences, IEEE Trans. Inform. Theory 42 (1996) 256–260.
[7] A. Klapper, M. Goresky, Revealing information with partial period correlations, in: H. Imai, R.L. Rivest, T. Matsumoto (Eds.), Advances in Cryptology—ASIACRYPT '91, Lecture Notes in Computer Science, Vol. 739, Springer, Berlin, 1993, pp. 277–287.
[8] A. Klapper, M. Goresky, Partial period autocorrelations of geometric sequences, IEEE Trans. Inform. Theory 40 (1994) 494–502.
[9] R. Lidl, H. Niederreiter, Introduction to Finite Fields and their Applications, Rev. Edition, Cambridge University Press, Cambridge, 1994.
[10] H. Niederreiter, A. Winterhof, Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators, Acta Arith. 93 (2000) 387–399.
[11] I.M. Vinogradov, Elements of Number Theory, Dover Publ., New York, 1954.
[12] A. Winterhof, On the distribution of powers in finite fields, Finite Fields Appl. 4 (1998) 43–54.
[13] A. Winterhof, Some estimates for character sums and applications, Designs Codes Cryptogr. 22 (2001) 123–131.
[14] A. Winterhof, Incomplete additive character sums and applications, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications, Springer, Berlin, 2001, pp. 462–474.